PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 17/60, G06G 7/52, G06K 5/00, H04K 1/10 — A1

(11) International Publication Number: **WO 96/29667**

(43) International Publication Date: 26 September 1996 (26.09.96)

(21) International Application Number: PCT/US96/03716

(22) International Filing Date: 19 March 1996 (19.03.96)

(30) Priority Data:
08/407,503 20 March 1995 (20.03.95) US

(60) Parent Application or Grant
(63) Related by Continuation
US 08/407,503 (CIP)
Filed on 20 March 1995 (20.03.95)

(71)(72) Applicant and Inventor: SANDBERG-DIMENT, Erik [US/US]; 699 Pomfret Road, Hampton, CT 06247 (US).

(74) Agent: FEIGENBAUM, David, L.; Fish & Richardson P.C., 225 Franklin Street, Boston, MA 02110-2804 (US).

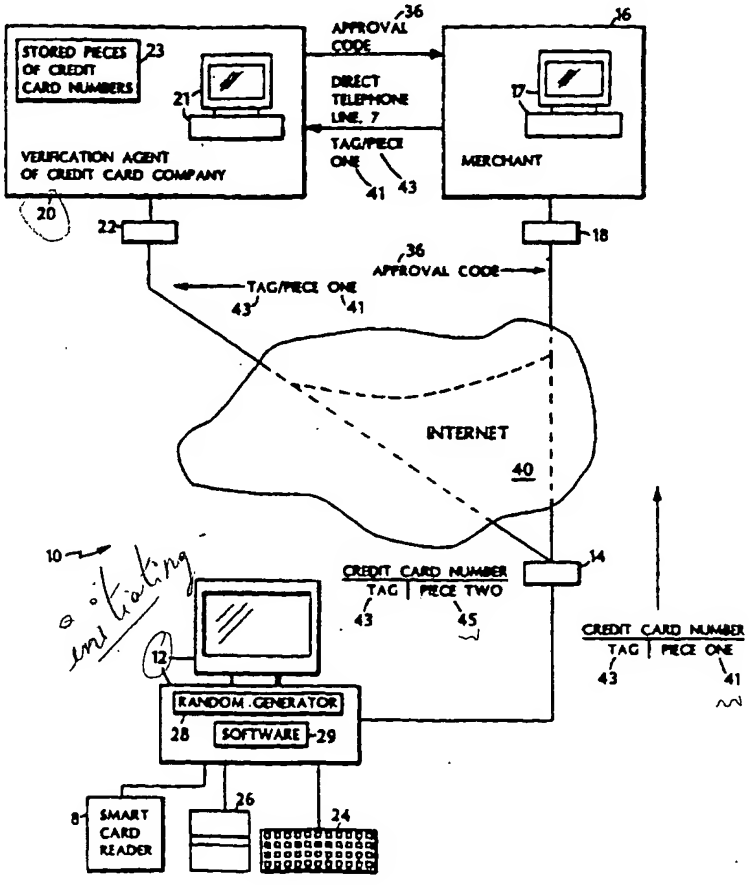
(81) Designated States: AL, AM, AT, AU, AZ, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, US, UZ, VN, ARIPO patent (KE, LS, MW, SD, SZ, UG), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: PROVIDING VERIFICATION INFORMATION FOR A TRANSACTION

(57) Abstract

Verification information is provided with respect to a transaction between an initiating party (12) and a verification-seeking party (16), the verification information being given by a third, verifying party (20), based on confidential information in the possession of the initiating party. On behalf of the initiating party, first and second tokens (41, 45) are generated, each of which represents some but not all of the confidential information. The first token is sent electronically via a nonsecure communication network (40) from the initiating party to the verifying party. Verification information is sent electronically via a nonsecure communication network from the verifying party to the verification-seeking party. In another aspect, different pieces of a message may be deliberately sent by different routes to reduce the chances of the pieces all being picked up at a node along the route.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia	**GB**	United Kingdom	**MW**	Malawi
AT	Austria	**GE**	Georgia	**MX**	Mexico
AU	Australia	**GN**	Guinea	**NE**	Niger
BB	Barbados	**GR**	Greece	**NL**	Netherlands
BE	Belgium	**HU**	Hungary	**NO**	Norway
BF	Burkina Faso	**IE**	Ireland	**NZ**	New Zealand
BG	Bulgaria	**IT**	Italy	**PL**	Poland
BJ	Benin	**JP**	Japan	**PT**	Portugal
BR	Brazil	**KE**	Kenya	**RO**	Romania
BY	Belarus	**KG**	Kyrgystan	**RU**	Russian Federation
CA	Canada	**KP**	Democratic People's Republic of Korea	**SD**	Sudan
CF	Central African Republic			**SE**	Sweden
CG	Congo	**KR**	Republic of Korea	**SG**	Singapore
CH	Switzerland	**KZ**	Kazakhstan	**SI**	Slovenia
CI	Côte d'Ivoire	**LI**	Liechtenstein	**SK**	Slovakia
CM	Cameroon	**LK**	Sri Lanka	**SN**	Senegal
CN	China	**LR**	Liberia	**SZ**	Swaziland
CS	Czechoslovakia	**LT**	Lithuania	**TD**	Chad
CZ	Czech Republic	**LU**	Luxembourg	**TG**	Togo
DE	Germany	**LV**	Latvia	**TJ**	Tajikistan
DK	Denmark	**MC**	Monaco	**TT**	Trinidad and Tobago
EE	Estonia	**MD**	Republic of Moldova	**UA**	Ukraine
ES	Spain	**MG**	Madagascar	**UG**	Uganda
FI	Finland	**ML**	Mali	**US**	United States of America
FR	France	**MN**	Mongolia	**UZ**	Uzbekistan
GA	Gabon	**MR**	Mauritania	**VN**	Viet Nam

PROVIDING VERIFICATION INFORMATION FOR A TRANSACTION

Background

This invention relates to providing verification information for a transaction.

For example, as seen in Figure 1, a consumer at a remote terminal 12 in a network 10 may electronically make a credit card purchase from a merchant 16 by entering a credit card number 25 and expiration date 27 of the credit card through a keyboard 24 or a swiping device 26 (which reads an encoded metallic stripe on the card) attached to the terminal 12. Alternatively, a "smart" credit card with a built-in programmable microchip may be read by a smart card reader 8. The credit card number and expiration date may be transmitted along with the consumer's purchase order 9 (which has also been entered into the terminal) over unsecure telephone lines 31 (via the switched public telephone network 33) between the terminal's modem 14 and the merchant's modem 18. At the merchant's end, a terminal 17 receives the information and stores it pending verification. The merchant verifies the purchase by electronically transmitting from terminal 17 via modem 18 and via the switched public telephone network 33 the credit card number 25 and the price of the order to a terminal 21 at the verification agent of the consumer's credit card company 20 via its modem 22. The merchant's terminal 17 receives back from the verification agent's terminal 21 an authorization code 36 which guarantees payment from the credit card company. The merchant then ships the goods.

Summary

The invention provides a way to pass confidential information over an unsecured network with reduced risk of it being captured by an untrusted party.

Thus, in general, in one aspect, the invention features a method and apparatus for giving verification information with respect to a transaction between an initiating party and a verification-seeking party, the verification information being given by a third, verifying party, based on confidential information in the possession of the initiating party. On behalf of the initiating party, first and second tokens are generated, each of which represents some but not all of the confidential information. The first token is sent electronically via a nonsecure communication network from the initiating party to the verification-seeking party. The second token is sent electronically via a nonsecure communication network from the initiating party to the verifying party. The confidential information is verified at the verifying party based on the first and second tokens. Verification information is sent electronically via a nonsecure communication network from the verifying party to the verification-seeking party.

Implementations of the invention may include one or more of the following features. At least some of the confidential information may be stored at the verifying party. The verifying may be done by comparing the information represented by the first and second tokens with at least some of the stored confidential information. The tokens together may represent all of the confidential information. The tokens may include tags identifying the tokens as being related. The tags may be identical and may be randomly generated. The verifying may include associating the tokens with each other based on the tags. The tokens may include actual

pieces of the confidential information, and an indication of the order that the two pieces occupy in the confidential information. The two tokens may be of essentially equal size. The tokens need not be sent from the initiating party one immediately after the other. The confidential information may include an identification number, e.g., a credit card number. The transaction may include a purchase, the initiating party may be a consumer, the verifying party may be a verification agent of a credit card company, and the verification-seeking party may be a merchant. Additional non-confidential information related to the transaction may be sent from the initiating party to the verification-seeking party. The additional information may include an expiration date of a credit card and a purchase order.

In general, in another aspect, the invention features sending a digital message from a source to a destination via a packet switching network. The message is split into pieces that are sent from the source to the destination in different ones of a set of packets. The routing of different ones of the packets is controlled to reduce the likelihood of the different packets traveling together or via the same route. In implementations of the invention, the message may include a credit card number and the pieces may include portions of the number. The controlling may be done at the source.

Advantages of the invention may include one or more of the following. The confidential information may be sent via non-secure communications links because the entire block of confidential information (e.g., the credit card number) is not available on any one link at a given time. It is only available as an entire block in the hands of the initiator (e.g., the credit card holder)

and the verifying agent, and not to the verification-seeking party (e.g., a merchant).

Other advantages and features of the invention will become apparent from the following description and from the claims.

Description

Figures 1, 2, and 4 are block diagrams of terminals and a network.

Figure 3 is a flow diagram showing changes in data sent in a nonsecure communication network for a secured credit card transaction.

As seen in Fig. 2, to provide security in the transmission of a credit card number over an open network including, for example, the Internet 40, in connection with a purchase transaction, the credit card number may be split into two pieces. Only one piece 41 is sent to the merchant 16, and the other 45 is sent to the verification agent 20. An identification tag 43 is attached to each piece to permit later identification and reassembly of the credit card number by the verification agent 20. After the merchant 16 has received the consumer's order, the card expiration date, the tagged piece of the credit card number, and the price of the order are sent to the verification agent 20 via the Internet 40. The verification agent 20 combines the tagged pieces of the credit card number to reconstruct the number, checks the consumer's credit, and issues an approval code 36 to the merchant 16. In this process, only the customer and the verification agent 20 ever have possession of the complete credit card number.

Referring also to Fig. 3, the process begins when the consumer enters his credit card number 30 (e.g., a ten digit string), the expiration date of the credit card, and a purchase order (step 100). Software 29 (Fig. 2) running on computer 12 splits the number 30 into the

two pieces 32a and 32b, e.g., two pieces of equal length (each five digits) (step 102). The software 29 also stores the network addresses of the merchant 16 and the verification agent 20. Alternatively, a smart credit card with a microchip may contain the accessing software and information such as the relevant network addresses.

The software 29 includes a random number or character generator 28 which issues a four-digit pseudorandom tag 34 (step 104). The same tag 34 is added to both pieces 32a and 32b of the credit card number (step 106). The random tag 34 is attached to the end of one piece 32a and to the beginning of the other piece 32b, so that the verification agent 20 may easily tell which piece comes first in reconstructing credit card number 30.

The pseudorandom tag 34 may contain more than four digits. The tag 34 may be distinguished from the number by introducing an alphabetic character into the tag or by separating the shorter tag from the longer number by a string of zeros. Use of a pseudorandom tag 34 reduces the chance that someone monitoring the output of the computer 12 for the purpose of attempting to steal the credit card number 30 will be able to predict which tag will be used.

Computer 12 sends two separate packages of information via modem 14. One package holds the first tagged piece 32a and is sent directly to the verification agent 20 at its network address (step 108). The verification agent 20 receives the tagged piece 32a via its modem 22, and stores the tagged piece 32a for later recall.

The other package holds the second tagged piece 32b and is sent over the network (step 110) to the merchant 16 at its network address, along with the consumer's purchase order (including the consumer's name

and address), credit card expiration date, and identification of the consumer's credit card company. The merchant's terminal may store the network address of the verification agent 20, or the address may be generated by computer 12 and sent to merchant 16 with the consumer's purchase order.

The two packages may be sent in either order. Allowing a time interval (of say 30 seconds) to pass between sending the two packages decreases the likelihood that both pieces 32a and 32b will be intercepted and recognized by their random tags (step 109).

Merchant 16 receives the tagged piece 32b and the other information at its modem 18 for storage and processing. The merchant 16 may prepare the consumer's order while waiting for an approval number from the verification agent 20. The merchant 16 does not know the consumer's entire credit card number 30, and for that and other reasons it must obtain approval from the verification agent 20 before it ships the consumer's order to ensure that it will receive payment. Accordingly, the merchant 16 sends piece 32b along with the price of the consumer's order from its modem 18 to the modem 22 of the verification agent 20 over the network 10 (step 112) or by direct telephone line 7 (Fig. 2) from the merchant 16 to the verification agent 20 outside the network 10.

The verification agent's terminal 21 compares the tag 34 of piece 32b to the tags of other pieces of credit card numbers 23 it has received over the network 10 (step 114). The tags in the pieces of credit card numbers received by the verification agent 20 are isolated by pattern recognition and matching or through a convention that the tag is always at the beginning or end of the number. When the tags 34 of two received pieces 32a and 32b are found to match, the verification agent 20 removes

the tag from the end of piece 32a and the tag from the beginning of piece 32b and recombines the pieces in that sequence to obtain the consumer's credit card number 30 (step 116).

The verification agent 20 may then perform a credit check on the consumer's account (step 118). If the purchase is approved, the verification agent 20 sends an approval code 36 to the merchant 16 over the network 10 or by the direct telephone line 7 between the verification agent 20 and the merchant 16 (step 120). Later, the merchant 16 will present the transaction for payment, including the tagged piece 32b, the approval code 36, the price, and an identification of the goods. The credit card company will debit the consumer's credit card account for the price of that order and credit the merchant's account. If the purchase is not approved, the merchant 16 is so notified and will refuse the consumer's purchase order.

Using this procedure, the merchant 16 never receives the entire credit card number 30, but rather only a tagged piece 32b and an approval code 36 which need not bear any relation to the credit card number 30 itself. The credit card number 30 is never available as a whole except at the consumer's computer 12 and at the verification agent 20.

The TCP/IP or ISO protocols used for packet transmission are designed to lead to the best routing of packets over the network. For this reason it is likely that the two parts of, e.g., the credit card number carried in the two packets may be sent along the same route most of the way (they may even travel together, one after the other) and therefore pass through the same nodes along the route. This may make it possible for someone at one of those nodes to collect all of the packets that make up the credit card number (or other

information) as they pass through the node, and thus to reassemble the credit card number.

To prevent this, it would be possible to add, to the software in the computer which is the originator of the packets that contain the pieces of the message, routines whose purpose is to configure the packets under the protocol in a way that makes it more likely (even highly likely or certain) that the packets will traverse different routes to their destinations as soon as they leave the originating computer. This could entail changing the route generation routines to assure different routes or different portions of routes. The changes could be made within a layer of the protocol or by addition of another layer. The objective would be to increase the likelihood or assure that packets associated with a given message do not travel together and/or do not take the same route through the network.

The same approach may be applied to any message that is to be or is susceptible to be broken into parts. The message could be broken down as individual words, or characters, or bytes, or even individual bits, with each piece carried in its own packet and the protocol reducing the likelihood that they will take the same paths or travel together. This would make the message highly secure even without encryption.

Thus, in Figure 4, the characters X of one piece of the consumer's credit card number would each be sent by a different route as would the characters Y of the other piece.

The controlling of the routing could be done in a way that assures divergent paths for only part of the routes to the destination and the controlling could be done in nodes downstream of the source node.

Other embodiments are within the scope of the following claims. The piece splitting may be used in

other kinds of financial transactions. The technique could be used in a wide range of applications to protect confidential information. Also, more than three parties could be involved. More than three pieces could be used. The method could be used with any unsecured communication medium.

What is claimed is:

Claims

1. A method for giving verification information with respect to a transaction between an initiating party and a verification-seeking party, the verification information being given by a third, verifying party, based on confidential information in the possession of the initiating party, the method comprising:

on behalf of the initiating party, generating first and second tokens each of which represents some but not all of the confidential information,

sending the first token electronically via a nonsecure communication network from the initiating party to the verification-seeking party,

sending the second token electronically via a nonsecure communication network from the initiating party to the verifying party,

verifying the confidential information at the verifying party based on the first and second tokens, and

sending the verification information electronically via a nonsecure communication network from the verifying party to the verification-seeking party.

2. The method of claim 1 further comprising

storing, at the verifying party, at least some of the confidential information, and wherein

the verifying is done at the verifying party by comparing the information represented by the first and second tokens with at least some of the stored confidential information.

3. The method of claim 1 wherein the first and second tokens together represent all of the confidential information.

4. The method of claim 1 wherein the first and second tokens include tags identifying the first and second tokens as being related.

5. The method of claim 4 wherein the tags in the two tokens are identical.

6. The method of claim 4 further comprising generating the tags randomly.

7. The method of claim 4 wherein the verifying comprises associating the first and second tokens with each other based on the tags.

8. The method of claim 1 wherein the tokens include

pieces of the confidential information, and

an indication of the order of the two pieces in the confidential information.

9. The method of claim 1 wherein the two tokens are of essentially equal size.

10. The method of claim 1 wherein the first token and the second token are not sent from the initiating party one immediately after the other.

11. The method of claim 1 wherein the confidential information comprises an identification number.

12. The method of claim 1 wherein the confidential information comprises a credit card number.

13. The method of claim 12 further comprising sending additional non-confidential information related to the transaction from the initiating party to the verification-seeking party.

14. The method of claim 13 wherein the additional information comprises an expiration date of a credit card.

15. The method of claim 13 wherein the additional information comprises a purchase order.

16. The method of claim 1 wherein the transaction comprises a purchase, the initiating party is a consumer, the verifying party is a verification agent of a credit card company, and the verification-seeking party is a merchant.

17. The method of claim 1 further comprising sending additional non-confidential information related to the transaction from the initiating party to the verification-seeking party.

18. The method of claim 17 wherein the additional information comprises an expiration date of a credit card.

19. The method of claim 17 wherein the additional information comprises a purchase order.

20. A method for enabling a consumer to conduct a credit card transaction with a merchant via an nonsecure communication medium comprising:

sending a first token electronically via the communication medium from the consumer to the merchant, the first token including a piece of a credit number of the consumer and a tag that identifies the first token,

sending a second token electronically via the communication medium from the consumer to a verification agent, the second token including a piece of the

consumer's credit number and a tag that identifies the second token,

the pieces of the consumer's credit number together incorporating all of the credit number,

the tags indicating an association of the two tokens with one another,

storing the consumer's credit number at the verification agent,

sending the first token electronically via the communication medium from the merchant to the verification agent, and

at the verification agent:

associating the first and second tokens based on the tags,

deriving the credit number from the tokens, and

sending verification information from the verification agent to the merchant.

21. A method for giving verification information with respect to a transaction between an initiating party and a responding party, the verification being given by a third, authorizing party, based on confidential information in the possession of the initiating party, the method comprising:

on behalf of the initiating party, generating first and second tokens each of which represents some but not all of the confidential information,

sending the first token electronically via a nonsecure communication network from the initiating party to the responding party,

sending the second token electronically via a nonsecure communication network from the initiating party to the authorizing party,

verifying the confidential information at the authorizing party based on the first and second tokens, and

sending verification information electronically via a nonsecure communication network from the authorizing party to the responding party.

22. A method for giving verification information with respect to a transaction between an initiating party and a verification-seeking party, the verification information being given by a third, verifying party, based on confidential information in the possession of the initiating party, the method comprising:

on behalf of the initiating party, generating first and second tokens each of which represents some but not all of the confidential information,

on behalf of the initiating party, sending the first and second tokens electronically via a nonsecure communication network,

collecting the first and second tokens at the verifying party,

verifying the confidential information at the verifying party based on the first and second tokens, and

sending the verification information electronically via a nonsecure communication network from the verifying party to the verification-seeking party.

23. A method for sending confidential information from an initiating party to a receiving party comprising:

on behalf of the initiating party, generating first and second tokens each of which represents some but not all of the confidential information,

sending the first token electronically via a nonsecure communication network from the initiating party to the receiving party,

sending the second token electronically via a nonsecure communication network to a remote destination which is not related to the initiating party and the receiving party,

sending the second token electronically via a nonsecure communication network from the remote destination to the receiving party, and

recovering the confidential information at the receiving party based on the first and second tokens.

24. A method of sending a digital message from a source to a destination via a packet switching network comprising

splitting the message into pieces,

sending each of the pieces from the source to the destination in a different one of a set of packets, and

controlling the routing of different ones of the packets to reduce the likelihood of the different packets traveling together or via the same route.

25. The method of claim 24 in which the message comprises a credit card number and the pieces comprise portions of the number.

26. The method of claim 24 in which the controlling is done at the source.

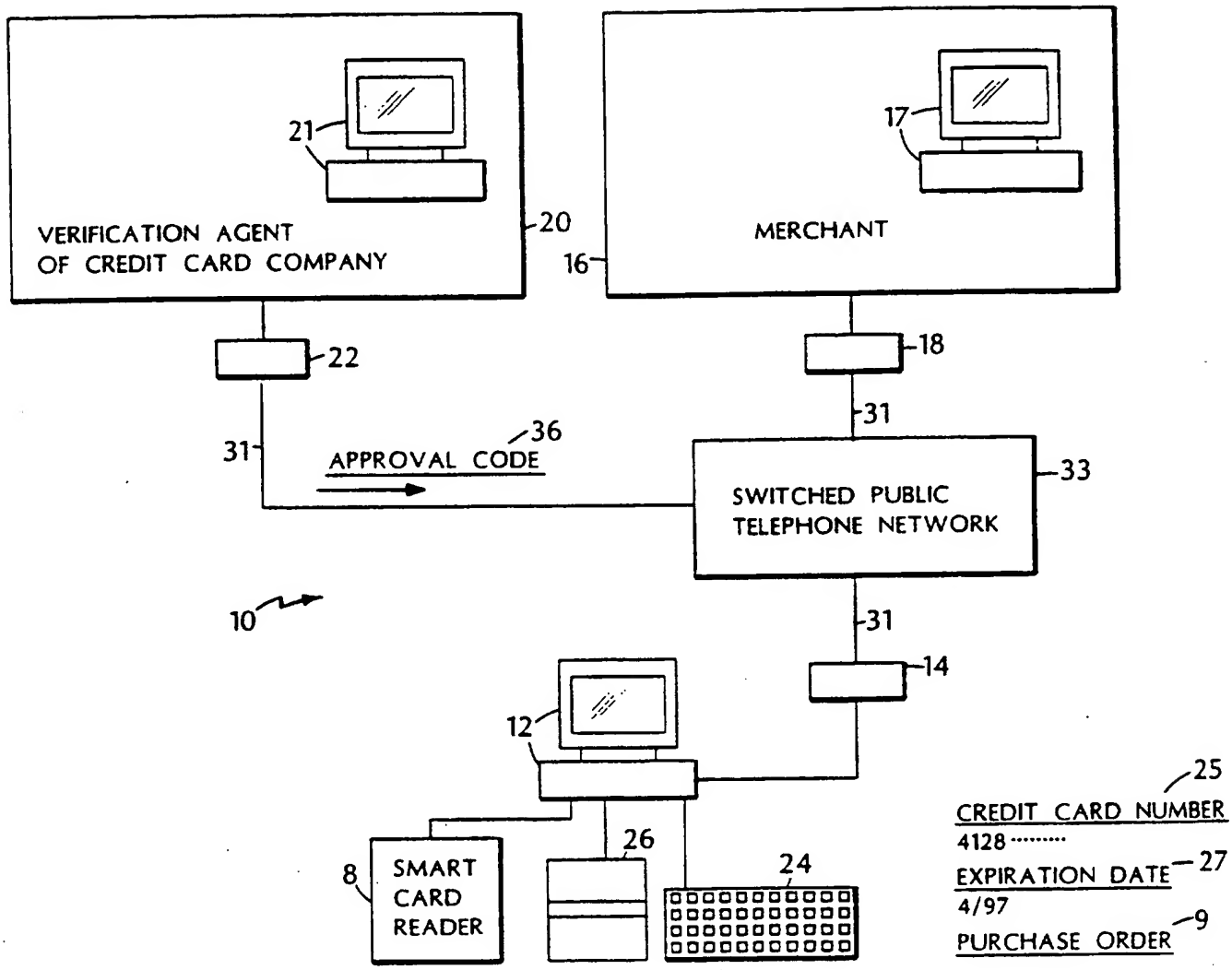

VERIFICATION AGENT
OF CREDIT CARD COMPANY
21
20
MERCHANT
17
16
22
18
31
36
APPROVAL CODE
31
SWITCHED PUBLIC
TELEPHONE NETWORK
33
10
31
14
12
25
CREDIT CARD NUMBER
4128 .....
EXPIRATION DATE
27
4/97
PURCHASE ORDER
9
8
SMART
CARD
READER
26
24

FIG. 1

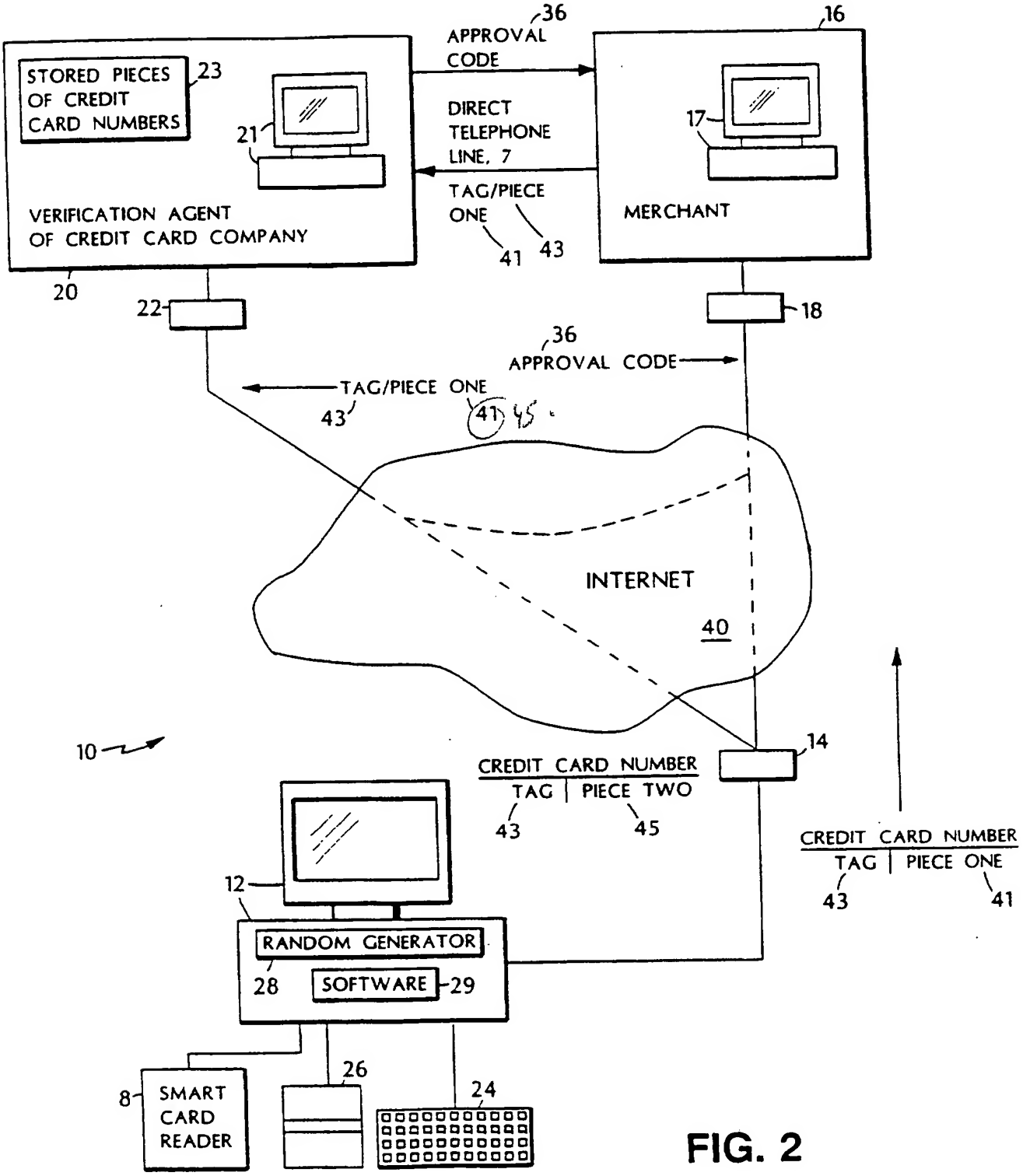

36
APPROVAL CODE
16
STORED PIECES OF CREDIT CARD NUMBERS
23
21
DIRECT TELEPHONE LINE, 7
17
TAG/PIECE ONE
41
43
VERIFICATION AGENT OF CREDIT CARD COMPANY
MERCHANT
20
22
18
36
APPROVAL CODE
TAG/PIECE ONE
43
41
45
INTERNET
40
10
14
CREDIT CARD NUMBER
TAG | PIECE TWO
43
45
CREDIT CARD NUMBER
TAG | PIECE ONE
43
41
12
RANDOM GENERATOR
28
SOFTWARE
29
8
SMART CARD READER
26
24

FIG. 2

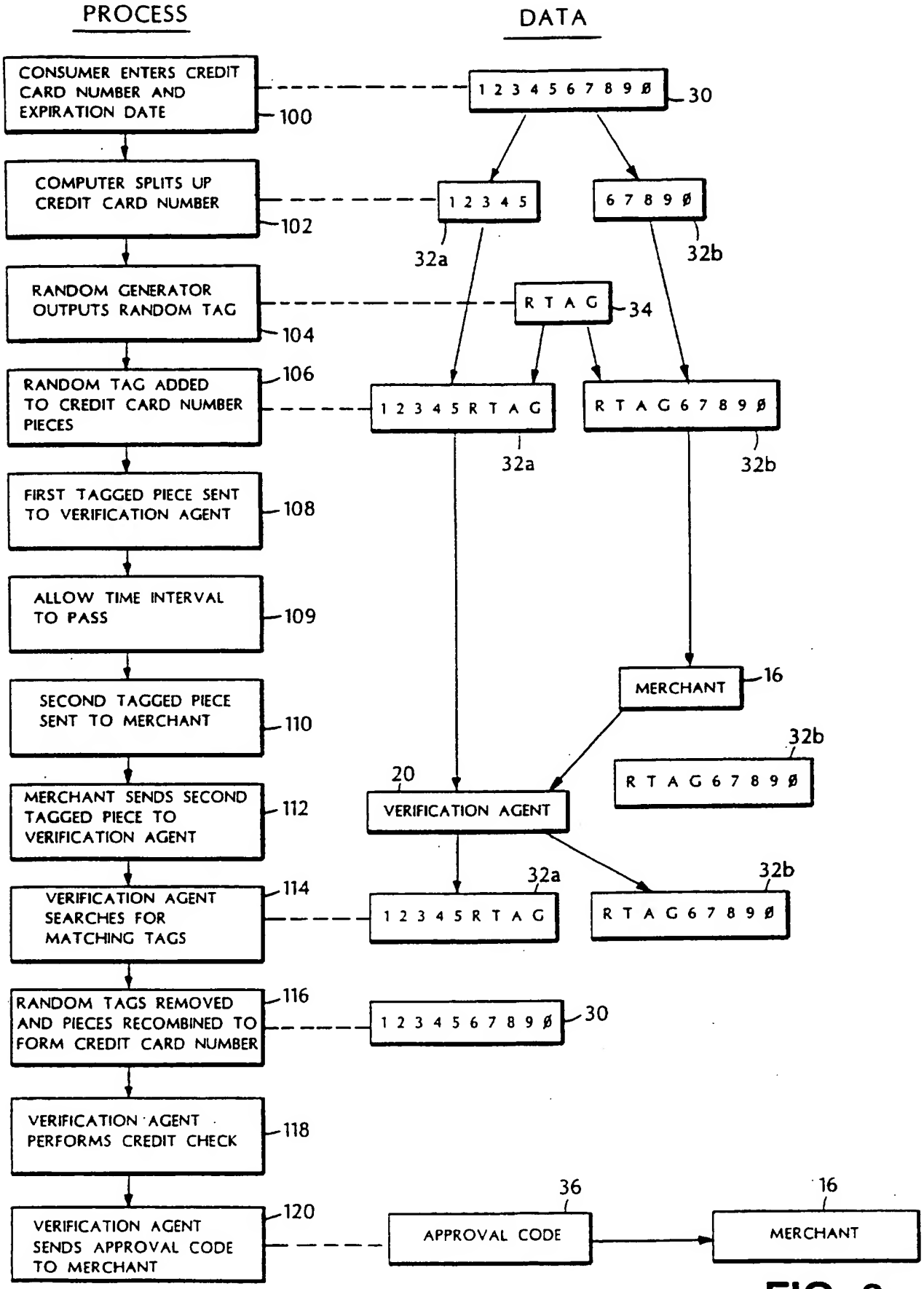

PROCESS
DATA
CONSUMER ENTERS CREDIT CARD NUMBER AND EXPIRATION DATE
100
1 2 3 4 5 6 7 8 9 Ø
30
COMPUTER SPLITS UP CREDIT CARD NUMBER
102
1 2 3 4 5
6 7 8 9 Ø
32a
32b
RANDOM GENERATOR OUTPUTS RANDOM TAG
104
R T A G
34
RANDOM TAG ADDED TO CREDIT CARD NUMBER PIECES
106
1 2 3 4 5 R T A G
R T A G 6 7 8 9 Ø
32a
32b
FIRST TAGGED PIECE SENT TO VERIFICATION AGENT
108
ALLOW TIME INTERVAL TO PASS
109
SECOND TAGGED PIECE SENT TO MERCHANT
110
MERCHANT
16
32b
R T A G 6 7 8 9 Ø
20
MERCHANT SENDS SECOND TAGGED PIECE TO VERIFICATION AGENT
112
VERIFICATION AGENT
VERIFICATION AGENT SEARCHES FOR MATCHING TAGS
114
32a
1 2 3 4 5 R T A G
32b
R T A G 6 7 8 9 Ø
RANDOM TAGS REMOVED AND PIECES RECOMBINED TO FORM CREDIT CARD NUMBER
116
1 2 3 4 5 6 7 8 9 Ø
30
VERIFICATION AGENT PERFORMS CREDIT CHECK
118
VERIFICATION AGENT SENDS APPROVAL CODE TO MERCHANT
120
36
APPROVAL CODE
16
MERCHANT

FIG. 3

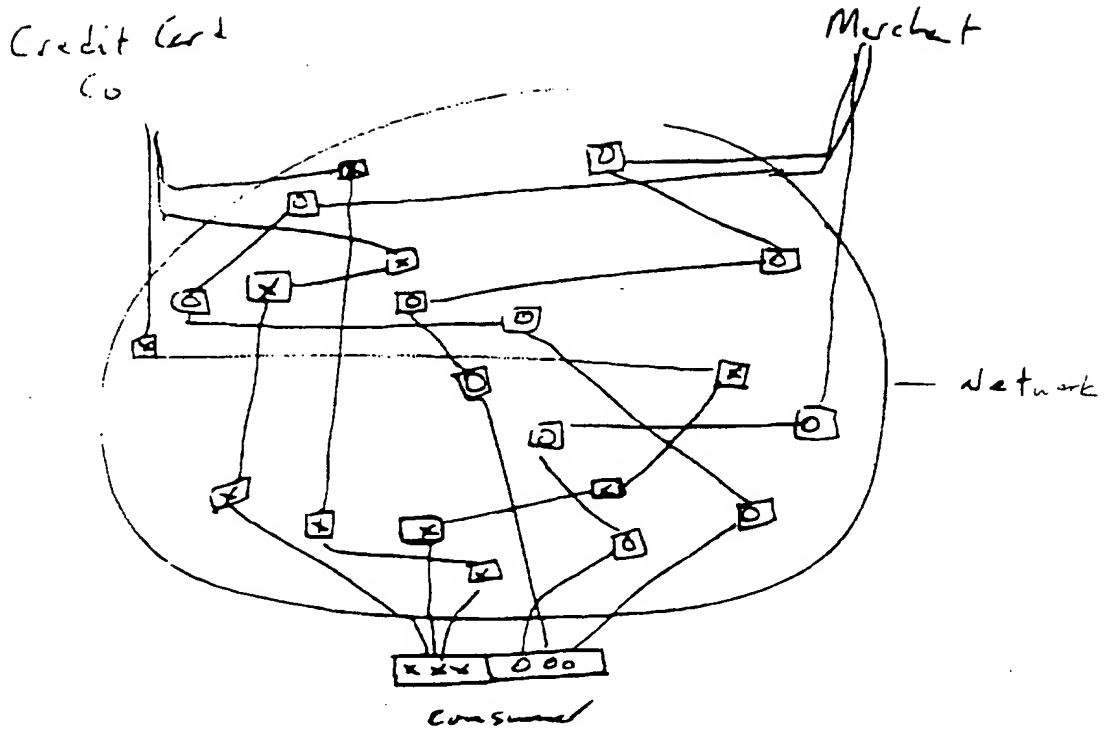


FIGURE 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US96/03716

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :G06F 17/60; G06G 7/52; G06K 5/00; H04K 1/10
US CL :364/408, 401; 235/375, 380, 381; 380/33
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 364/408, 401; 235/375, 380, 381; 380/23, 24, 25, 33, 49

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

Please See Extra Sheet.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US, A, 4,498,000 (DECAVELE et al.) 05 FEBRUARY 1985 see entire document	1-26
A	US, A, 4,679,236 (DAVIES) 07 JULY 1987 see entire document	1-26

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be part of particular relevance

"E" earlier document published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
09 JUNE 1996	02 JUL 1996
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231	Authorized officer DONALD E. MCELHENY JR.
Facsimile No. (703) 305-3230	Telephone No. (703) 305-3800

Form PCT/ISA/210 (second sheet)(July 1992)★

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US96/03716

B. FIELDS SEARCHED
Electronic data bases consulted (Name of data base and where practicable terms used):

APS
search terms: third party, verifi?, verify?, authoriz?, partial, part, parts, token#, tag#

DIALOG
search terms: thirs party, verifi?, verify?, authoriz?, partial, part, parts, credit card, internet